Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	8	709/204.ccls. and (instant adj messag$) and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:14
L2	39	(instant adj messag$) and presence and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:14
L3	8	709/203,204,206,207.ccls. and ((instant adj messag$) and presence) and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:15
L4	3	(instant adj messag$) and presence.ab. and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:15
L5	20	(instant adj messag$) and presence.ab.	USPAT	OR	OFF	2005/08/21 16:15
L6	2	((internet or www) and (conferenc$ or meet$ or collaborat$).ab.) and (status).ab. and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:15
L7	0	instant with mess$8 same presence and (master or main or head or primary or lead$3) with status and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:15
L8	1	(master adj status) same (invisible or stealth or block) and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:16
L9	2	((internet or www) and (conferenc$ or meet$ or collaborat$).ab.) and (status).ab. and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:16
L10	73	presence.ti. and status.ab. and @pd>"20050219"	US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/08/21 16:16
L11	1	instant with mess$8 same presence and (master or main or head or primary or lead$3) with (status or rank or place or position or rat$4 or state or qualification) and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:17
L12	4	(one or single or lone or solitary or sole) with (customer or user or client) same (multiple or (more with one) or different or two or three or four or five or many or several or numerous or various or diverse or (more near3 'or')) same (station or computer or system or laptop or desktop) and (presence and (status or messag$4)).ab. and @pd>"20050219"	USPAT	OR	OFF	2005/08/21 16:17

```
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200553
         (c) 2005  Thomson Derwent

Set     Items   Description
S1      87679   (MULTIPLE OR MULTIPLICITY OR PLURAL? OR TWO OR SECOND??? OR
              2ND)(3W)(COMPUTER? ? OR PC? ? OR CLIENT? ? OR TERMINAL? ? OR
             WORKSTATION? ? OR WORK()STATION? ? OR NODE? ?)
S2      70817   (DUAL OR BOTH OR DIFFERENT OR MORE()(THEN OR THAN) OR MANY
             OR ANOTHER OR OTHER)(3W)(COMPUTER? ? OR PC? ? OR CLIENT? ? OR
             TERMINAL? ? OR WORKSTATION? ? OR WORK()STATION? ? OR NODE? ?)
S3         91   (LOG? ? OR LOGGED OR LOGGING OR SIGN? ? OR SIGNED OR SIGNI-
             NG)()(INTO OR IN OR ONTO OR ON)(7N)S1:S2
S4     717405   NETWORK? ? OR LAN OR DOMAIN? ? OR SERVER? ? OR INTERNET OR
             WEB
S5    4429872   STATUS OR STATE OR LOCATION OR POSITION OR PRESENCE
S6         12   S3 AND S4 AND S5
S7          1   CONCURRENT()LOGIN? ?
S8         10   (CONCURREN? OR SIMULTANEOUS)(5N)(LOGIN? ? OR LOGON? ?)
S9         62   (LOG? ? OR LOGGED OR LOGGING OR SIGN? ? OR SIGNED OR SIGNI-
             NG)()(INTO OR IN OR ONTO OR ON)(7N)(SIMULTANEOUS? OR CONCURRE-
             N?)
S10        26   S4 AND S9
S11        25   S10 NOT S8
```

```
File   8:Ei Compendex(R) 1970-2005/Aug W1
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Jul
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Aug W2
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Aug W1
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Jun W4
         (c)2005 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2005/Aug W1
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Aug W1
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Aug W2
         (c) 2005 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jul
         (c) 2005 The HW Wilson Co.
File 266:FEDRIP 2005/Jun
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2005/Jul W2
         (c) 2005 FIZ TECHNIK
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 438:Library Lit. & Info. Science 1984-2005/Jul
         (c) 2005 The HW Wilson Co
File 256:TecInfoSource 82-2005/Jul
         (c) 2005 Info.Sources Inc

Set     Items   Description
S1      69755   (MULTIPLE OR MULTIPLICITY OR PLURAL? OR TWO OR SECOND??? OR
              2ND)(3W)(COMPUTER? ? OR PC? ? OR CLIENT? ? OR TERMINAL? ? OR
             WORKSTATION? ? OR WORK()STATION? ? OR NODE? ?)
S2      87055   (DUAL OR BOTH OR DIFFERENT OR MORE()(THEN OR THAN) OR MANY
             OR ANOTHER OR OTHER)(3W)(COMPUTER? ? OR PC? ? OR CLIENT? ? OR
             TERMINAL? ? OR WORKSTATION? ? OR WORK()STATION? ? OR NODE? ?)
S3         35   (LOG? ? OR LOGGED OR LOGGING OR SIGN? ? OR SIGNED OR SIGNI-
             NG)()(INTO OR IN OR ONTO OR ON)(7N)S1:S2
S4    3959441   NETWORK? ? OR LAN OR DOMAIN? ? OR SERVER? ? OR INTERNET OR
             WEB
S5    7899910   STATUS OR STATE OR LOCATION OR POSITION OR PRESENCE
S6         31   RD S3 (unique items)
```

```
File 275:Gale Group Computer DB(TM) 1983-2005/Aug 19
         (c) 2005 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Aug 19
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Aug 18
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Aug 18
         (c) 2005 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2005/Aug 18
         (c)2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Aug 18
         (c) 2005 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2005/Aug 18
         (c) 2005 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2005/Jul W5
         (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Aug W1
         (c) 2005 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2005/Aug 18
         (c) 2005 Dialog
File 369:New Scientist 1994-2005/May W5
         (c) 2005 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2005/Aug 19
         (c) 2005 Business Wire.
File 613:PR Newswire 1999-2005/Aug 19
         (c) 2005 PR Newswire Association Inc

Set     Items   Description
S1     218082   (MULTIPLE OR MULTIPLICITY OR PLURAL? OR TWO OR SECOND??? OR
              2ND)(3W)(COMPUTER? ? OR PC? ? OR CLIENT? ? OR TERMINAL? ? OR
             WORKSTATION? ? OR WORK()STATION? ? OR NODE? ?)
S2     784194   (DUAL OR BOTH OR DIFFERENT OR MORE()(THEN OR THAN) OR MANY
             OR ANOTHER OR OTHER)(3W)(COMPUTER? ? OR PC? ? OR CLIENT? ? OR
             TERMINAL? ? OR WORKSTATION? ? OR WORK()STATION? ? OR NODE? ?)
S3       1768   (LOG? ? OR LOGGED OR LOGGING OR SIGN? ? OR SIGNED OR SIGNI-
             NG)()(INTO OR IN OR ONTO OR ON)(7N)S1:S2
S4   14052741   NETWORK? ? OR LAN OR DOMAIN? ? OR SERVER? ? OR INTERNET OR
             WEB
S5   10639146   STATUS OR STATE OR LOCATION OR POSITION OR PRESENCE
S6         18   S3(7N)(SAME()TIME)
S7         11   RD (unique items)
S8        102   S3(50N)S4(50N)S5
S9         67   RD (unique items)
S10        48   S9 NOT (S7 OR PY=2001:2005)
S11         0   (FUTURUS OR HUDSON) AND ROAMING()USER()PROFILES
```

7/9/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01861495 SUPPLIER NUMBER: 17433066 (THIS IS THE FULL TEXT)
All quiet on the NetWare front. (how to secure four weak areas on NetWare networks)(Special Report) (Product Support)(Tutorial)
Runyan, Pete
LAN Magazine, p142(6)
Oct, 1995
DOCUMENT TYPE: Tutorial ISSN: 1069-5621 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4939 LINE COUNT: 00401

ABSTRACT: Security on NetWare networks involves four levels: login security, file server, rights and attribute security. Login security refers to the primary level of access. Simple login security can be established when setting up user accounts. Setting the Force Periodic Password Changes option is a good idea. Upon installing NetWare, two accounts are created, and when setting up a new server, passwords for the Guest and Supervisor accounts should be set immediately. Securing the file server console is fairly simple using the RCONSOLE utility. Rights security occurs through the use of trustee assignments. Several NetWare tools are able to manipulate trustee assignments.

TEXT:

Understanding how NetWare handles security will help you meet the responsibility of keeping your network safe from attack. Here's how to lock up the four vulnerable areas of your NetWare network.

If, as a network administrator, you haven't yet been besieged with security problems, consider yourself lucky. Network security is being pushed to the front of administration priorities as users become more computer literate, the number and use of networks continue to grow, and the tools for analyzing how a network functions become more sophisticated and easy to use. It seems safe to say that if your organization doesn't have strict security needs now, it probably will in the future.

For this article, let's assume the worst: Your network environment is rife with hostile or criminal elements. You need security, and you want it tight. Security risks are everywhere, and you want to use every tool NetWare provides to lock down your network tightly. If you're just setting up a NetWare network, you're in luck. It's always easier to establish good security measures when you're setting up a network, rather than backtrack herding the cows back into the barn because the doors were left open. If you have a well-established network of any size, the job is harder and longer, but still worth your efforts.

Traditionally, NetWare 3.11 security is broken down into four basic areas: login, file server, rights, and attribute security.

WHO KNOCKS?

Login security is concerned with the first level of security your network has: access. It's that simple. Your security worries are going to be greatly reduced if you can assure yourself that only users who have legitimate access to your network can log in to it.

First, you can establish simple login security when you set up your user accounts. Most of this work can be done in the NetWare utility SYSCON, which lets you create accounts, passwords, station restrictions, time restrictions, and account restrictions.

The place to start in SYSCON is under the Supervisor Options selection in the opening menu. The Default Account Balance/Restrictions option lets you set the following default values for all new accounts you create on your server after you have set the default values. Existing accounts will have to be changed manually if you choose to match them to any changes you make to the defaults. The main value you can set is Require Passwords, which defaults to No. Choose Yes to require that all users on the network log in using passwords and account names. Once this is done, you can set a minimum length for valid passwords. The default is five characters.

You can also set the Force Periodic Password Changes option. Choosing

Yes forces your users to change their passwords at a regular interval that you choose. You set the interval in the Days Between Forced Changes field. The NetWare default for this option is 40 days, but use your personal judgment for this one. (My users would riot if I made them change their passwords every 40 days.)

Once you have turned on the Require Passwords option you also have to decide whether to limit the number of grace logins. Grace logins are logins that access the network using an expired account password. The default is six. I feel that's a bit generous, so I set mine at five. Users whose account passwords have expired receive a message stating the number of remaining grace logins every time he or she attempts to log in. They will be asked if they wish to change their password. If they choose not to, they will use a grace login. Once their grace logins are all used, they will no longer be able to log in to the network.

Another option is Require Unique Passwords. NetWare automatically sets this to Yes when Yes is also chosen for the Require Password field. It forces users to select new passwords that are different from the ones they used previously. Setting this to No defeats the purpose of requiring password changes in the first place, so leave it set to Yes.

The next security option under the Supervisor Options menu is Default Time Restrictions. This setting allows you to control what days of the week and what times of the day a user can log in. Remember, you're setting a default value for all new accounts you create, so be careful. The NetWare default is to ignore time restrictions and allow login access 24 hours a day, seven days a week, for all users. If you have large numbers of users who will need to be restricted from the network at certain times--outside of normal business hours or on weekends, for example, then remove options for those days of the week and times of day.

The next option is File Server Console Operators, which I'll address in the upcoming section on file server security. However, this option contains the Intruder Detection/Lockout option, which is very important to login security. With this option, you can decide whether NetWare should be concerned with incorrect login attempts. NetWare's default is No. When you set this to Yes, you'll activate all of the fields on this screen, and NetWare will automatically keep track of "intruders"--anyone who makes a number of unsuccessful login attempts equal to the number specified in the Incorrect Login Attempts field.

Incorrect Login Attempts, then, sets the threshold value for defining an intruder. I give my users three attempts, figuring that even the most fumble-fingered person can type in his or her password in three attempts. NetWare's default for this field is seven.

The Bad Login Count Retention Time field controls how long NetWare "remembers" bad login attempts. The default for this field is 30 minutes if detection is activated. Lock Account After Detection determines whether or not a user who has achieved "intruder" status--that is, surpassed the acceptable number of login attempts--is denied access to the network. Again, NetWare will default to Yes if detection has been chosen. Length of Account Lockout controls how long a user is denied login permission once his or her account is locked. NetWare's default is 15 minutes, far too short an interval, assuming there is a real intruder.

After you have the defaults for your network established, go to the User Information option under the SYSCON main menu to create new accounts with your default settings or to alter existing accounts. Once you choose an existing user account (or create a new account) you can set Account Restrictions. Password options (they are the same ones covered in the previous Default Account section) are entirely customizable for each user, but the defaults are entered to save an administrator from establishing them separately for each new account. You can also disable the account with this option, which is handy in situations where you would like to ensure that the account is not used but don't want to remove it entirely. An employee going on vacation is a typical example of where you might use Account Disabled.

Finally, using Limit Concurrent Connections, you can set a value for the number of **different workstations** one user can **log in** from at the **same time** . NetWare places no restrictions on concurrent logins by

default. I recommend no more than two concurrent logins for your users. If you really want to tie a specific user to a specific computer, set this to one.

The Time Restrictions option lets you customize the daily and weekly login times for each user you select. In addition, User Information gives you a few new security options: Station Restrictions and Security Equivalences. Again, I'll save Security Equivalences for the discussion of security rights.

The Station Restrictions setting allows you to tie login access for a NetWare user account to a single workstation on your network. It requires you to enter your network's external identification number and the unique 12-digit address of the Ethernet card used by the computer you wish to fie the user to. Both of these values can be obtained by using the USERLIST NetWare command with the /A switch. Once set, the user cannot log in from any other workstation on your network. You can allow access from more than one workstation by entering the appropriate information.

BE ACCOUNT-ABLE

The two accounts created when you install NetWare (Guest and Supervisor) have no passwords. If you're setting up a new server, you should set up passwords for them immediately using SYSCON.

You should be cautious in your use of the Supervisor account. Use Supervisor to perform tasks that require supervisor privilege, and use a different account for regular use. This may seem inefficient, but a simple command that you might use as a regular user could have devastating consequences for your network if you are using Supervisor or have granted your regular account supervisor security equivalence--which is something else that should also be avoided.

I also recommend that you disable or delete the Guest account (it's created by default when you install NetWare). Novell's reason for creating the Guest account is to allow printing on a nondefault server. Guest is a very restricted account by default, but it's still known as a default account to anyone with much NetWare experience, and the goal here is to keep users who have no business on your server from accessing it at all. You can always create an account that is equivalent to Guest to allow nonregular users restricted access to your server if need be, and give users its account name and password on an as-needed basis.

You might not think of account names as being important to network security, but they are. Last names (or variations thereof) usually make more secure account names than first names because they're less common and harder to guess. An extra letter or number in combination with a last name will make guessing a correct account name much more difficult.

Note that the NetWare LOGIN.EXE program is sneaky: If you enter an invalid account name when logging in, LOGIN.EXE does not tell you it's invalid--it just goes ahead and prompts you for a password, and then fails your login attempt after the password has been entered. This makes it much haMMer for an intruder to guess an account name because there is no instant verification that one has been successfully discovered.

Stick with NetWare's default of at least five characters for account passwords, and when you assign a password to a user account, make it a random combination of letters and numbers. Again, it's much harder to guess, and it's much harder to pick up and remember by watching a legitimate user log in.

Workgroup Managers are specified users within NetWare who perform a function equivalent to an assistant supervisor account. They are usually designated to handle a specific user area of your network--the sales department, for example. These accounts have the ability to create and delete users and groups (but only those that they have created), and if the supervisor has assigned them file rights, they can assign trustee rights, volume restrictions, and disk-space restrictions to those accounts they have created.

As a result, you want to be very careful about who you make a workgroup manager, and you should probably give them a second account name to use for their regular network tasks. Workgroup managers cannot grant Supervisor security equivalence to accounts, create other workgroup managers, or modify their own login restrictions, unless they are managing

their own accounts.

Another recommendation is to flag all the files in your SYS:LOGIN directory as read-only. Because LOGIN.EXE resides here, if it is deleted or corrupted, users will not be able to log in.

Finally, it is possible to booby-trap your system login script to trap certain kinds of intruders. If you wanted to keep anyone who was trying to log in to your server from a different network cable segment, you could do so by branching them off to a command that automatically logs them off the network.

HANDS OFF THE CONTROLS

Securing your file server console is an absolute must--anyone with access to it can destroy your entire NetWare network in a very short time. Fortunately, file server console security is easy to implement.

The first step is to recognize that you will need access to the file server console, but that you don't have to be there physically to have access. Using the RCONSOLE NetWare utility, you can access the console from your desktop and perform all file server console tasks. Once you have configured the file server for RCONSOLE access by loading the NetWare Loadable Modules REMOTE.NLM and RSEX.NLM in your system's AUTOEXEC.NCF file, you can remove the keyboard and monitor from your file server. This prevents anyone who gains access to the server from doing any harm, unless they shut your server off--a minor offense compared to what they could do if they had access to the keyboard and could see what they were doing on the monitor. Don't forget to specify the RGONSOLE password when you load REMOTE.NLM, and make sure it isn't easy to guess. To be really cautious, you can physically lock your server in a closet somewhere.

Short of this, you can use the MONITOR.NLM'S Lock File Server Console feature to disable keyboard input at the console until the password you specify has been successfully entered. Under NetWare 3.11 you can also use the supervisor's password to unlock the keyboard.

The second step is to use NetWare's SECURE CONSOLE file server console command. Once SECURE CONSOLE has been invoked, you may load NLMs only from the SYS:SYSTEM directory. The idea here is to prevent anyone from loading a Trojan horse NLM from another directory.

SECURE CONSOLE also prevents the date and time from being changed on the file server, which is important because many of the security functions of NetWare depend on the accurate time-keeping of the server. It also bars entry into the operating system debugger, which a programmer could use to damage the network. Finally, it removes DOS from file server memory, preventing anyone from moving a damaging program to your server's DOS partition.

You should be very careful about assigning a user the "File Server Console Operator," privilege in SYSCON. Once granted, this user has the ability to run the NetWare FCONSOLE utility and perform a limited number of console tasks. These tasks include changing the system date and time, looking at current network connection information, enabling or disabling logins for users, or disabling the NetWare Transaction Tracking System, which is used to ensure database integrity.

DEAD TO RIGHTS

Rights security is implemented on your NetWare server by using trustee assignments in combination with NetWare's Inherited Rights Mask. Rights are special privileges that you give to users or user groups that allow them to perform specific functions on directories or files on your NetWare server. These functions include basic file tasks such as reading, writing, and copying, along with special NetWare uses, such as granting these capabilities to other users.

Once you have assigned a user or group one of these rights, they are said to be a trustee. It's a pretty safe bet that your users already have trustee assignments, because NetWare automatically places users you create in the group Everyone (unless you change the defaults), and Everyone has trustee assignments in SYS:PUBLIC and SYS:MAIL. Users are also granted a trustee assignment for their SYS:MAIL\USERID directory.

The eight NetWare trustee rights are listed in Table 1 (page 143). Note that they may have different functions depending on whether or not they are granted to a user or group on a specific directory, or to a file

within a directory.

The standard NetWare notation for rights shown using NetWare utilities such as RIGHTS or WHOAMI has the form SRWCEMFA (see Table 2, page 144). The presence of a right is indicated by the letter associated with it. A hyphen or blank space in place of a letter indicates that the right is absent. So, -RWCEMF- indicates that all rights except the supervisory right and Access Control are in effect, and S would indicate that only the supervisory right is in effect.

Performing common file and directory tasks (copying, renaming, deleting, listing directories, and so on) require certain NetWare rights. Some of the rights required may not be exactly what you might expect. Check Table 3 (page 146) for a list of what rights are required for each task.

TOOLS FOR TRUSTEES

NetWare provides several command-line tools for manipulating trustee assignments. GRANT allows you to add trustee rights to users or groups; REVOKE allows you to subtract trustee rights from users or groups; REMOVE allows you to delete a trustee assignment completely. You should know that even if you subtract all trustee rights using REVOKE, the user or group remains a trustee--albeit with no rights--until you use the REMOVE command to delete them from the directory or the file's trustee list.

You could use the menu-driven FILER and SYSCON utilities to perform trustee assignment tasks; and the NetWare Utilities reference manual gives in-depth explanations for both the menu-driven and command-line utilities.

Key to understanding how the Inherited Rights Mask functions with trustee assignments is the concept of flow-down rights. If you grant a user trustee Read and File Scan rights to a directory, they automatically inherit Read and File Scan rights in subdirectories of that directory. This is how NetWare trustee rights "flow-down" a directory structure.

But suppose you would like to restrict a user's ability to read files in subdirectories below the directory where a trustee assignment for the user has been made. This is where the Inherited Rights Mask comes in.

NetWare automatically establishes an Inherited Rights Mask (IRM) for each file and directory when they are created. The IRM uses the same eight rights as trustee assignments, and the default IRM for all files and directories is for all rights to be granted. The fact that all rights are granted in the IR by default doesn't mean that your users have all fights, however. In fact, NetWare ignores the IRM in the absence of trustee assignments. But the key here is understanding that it is the combination of explicitly assigned trustee rights that have flowed down and the rights allowed through the IRM that determine a user's final capabilities--called the user's effective rights--within a particular directory or file. This sounds more complicated than it is.

NetWare provides the Allow (command-line) and Filer (menu) utilities for modifying the IRM. To check your effective rights, use the command-line utilities recurs, NDIR, and WHOAMI, or use Filer.

Once you have these concepts and tools down, NetWare file and directory security starts to get interesting. The point you are concerned with for any user or user group is what effective rights they have with directories or files that are critical for your networks operation (files in SYS:SYSTEM, SYS:LOGIN, SYS:PUBLIC, SYS:MAIL, SYS:ETC, and any other critical program directories or files that you have created outside of NetWare's standard directories on the SYS: volume, for example).

To establish good file and directory security, you should know a few fundamental rules. First, if a user or group trustee is granted the supervisory right to a directory, it cannot be revoked at any subdirectory level below the one for which it was assigned. Because the supervisory right includes all rights, it can be dangerous. Therefore, you should grant it only in situations where the trustee in question needs total control over the entire directory tree below the directory where the supervisory right is granted.

Second, rights are additive. If a user in a group has both group trustee rights and user trustee rights to a directory or file, his effective rights will be the sum of both trustee assignments. Third, NetWare ignores the IRM in the absence of explicit trustee assignments. Fourth, the supervisory right assigned in the IRM has no effect unless the

user or group is granted the supervisory right with a trustee assignment.

Fifth, the IRM and the effective rights from a parent directory on a given directory or on a given file are overridden in the presence of an explicit trustee assignment made on that directory or on that file. The user or groups effective rights will be those granted by the trustee assignments. Conversely, if there are no explicit trustee assignments made for a user or group on a subdirectory or file below the point where a trustee assignment was made, the IRM determines which effective rights a user can inherit from the parent directory.

And sixth, to determine a user's effective rights in any particular file or directory, keep the following formula in mind. A user's effective rights are a combination of the effective rights that have flowed down from any directories above the one in which you are working, plus any explicit trustee assignments in the directory or file you are working in. They are filtered by any changes in the IRM for that directory or file.

CAVEATS FOR RIGHTS SECURITY

To simplify assignment of trustee rights and to keep the number of them at a minimum, I assign them by group whenever I can. Because NetWare automatically places all users in the group Everyone by default, I have kept that group, and assign trustee rights to it when I want to allow or disallow rights on a broad basis to my entire user community.

As was mentioned previously, NetWare assigns trustee rights to the group Everyone for SYS:PUBLIC and SYS:MAIL when you setup a server. Everyone has Read and File Scan rights in SYS:PUBLIC, and the Create right in SYS:MAIL This setup ensures that users can see and execute NetWare utilities they will need, and that users can create e-mail in each other's mail subdirectories off of SYS:MAIL. For this reason, again, make sure that each user on your server has a user login script in his or her SYS:MAIL\USERID directory to prevent someone from forging a user login script that might damage your network or a user's workstation. (Again, the Create right allows the creation of a file, but nothing else. So, if the user's login script is already in place, there is no way to create a new one or edit an existing one.)

If you have moved your standard NetWare utilities and user mail directories to locations other than the NetWare defaults, make sure that your security matches what NetWare establishes for defaults. Otherwise, you may leave your network wide open for problems and make things very difficult for your users because they won't have enough rights to see the new NetWare utility directories and other basic, important information.

When you create new user accounts, make sure that their home directories are secure, as well. Assign each user the supervisory right in his or her home directory. This allows the user complete control over a personal area. For generic network accounts such as Guest, disallow supervisory and Access Control rights in the home directory to contain any problems in a single area. Furthermore, concerning users' home directories, it's also a great idea to restrict the amount of volume space a user has access to using either the DSPACE or SYSCON utility. This prevents an individual user from hogging space on a volume. (If you are using only the SYS: volume, this is critical; if the SYS: volume runs out of space, your file server may crash.)

ATTRIBUTES IN NETWARE SECURITY

NetWare provides another layer of file and directory security beyond rights security. Attribute security is placed directly on files and directories. It overrides standard rights security in that you can use it to prevent access to directories or files that rights security would allow. Users can modify the attributes of a directory or file as long as they have the Modify right to it.

The standard NetWare tools used for modifying file or directory attributes are FLAG (command line) and Filer. Viewing the attributes to confirm they are in place is done using NDIR. As a general rule, I find that the command-line utilities are quicker to use once you are used to their syntax. The menu driven utilities take a while to wade through and aren't particularly intuitive.

NetWare sets all the files in SYS:SYSTEM, SYS:PUBLIC, and SYS:LOGIN as Read-Only, System, Delete Inhibit, and Rename Inhibit, in order to prevent

accidental (or intentional) deletion, copying, or renaming. Most major software packages recommend that you flag crucial application executables as read-only, but they may also require you to allow users to write temporary files to the directory where the software is installed. This means that you cannot simply deny users write access to the directory as a whole using trustee assignments or the IRM, and it illustrates the kind of balancing act you may find yourself facing as you install rights and attribute security on your server.

CLEARING YOUR CONSCIENCE

implementing security on your server can be a tricky affair. If you spend some time getting used to the concepts behind Novell's approach and then practice a bit, you should have no problem establishing security that meets your needs now, as well as the capability to easily modify your network as your security needs change in the future.